Группы доступа

Группы доступа предназначены для настройки прав и ограничений прав доступа конкретным пользователям и группам пользователей программы. В группе реквизитов «**Группы доступа**» подраздела «**Настройка пользователей и прав**» сгруппированы следующие команды и настройки:

- «**Группы доступа**» — настройка прав доступа и ограничений для пользователей и групп пользователей. Группа доступа определяет совокупность действий с данными программы, которые могут выполнять участники этой группы;
- «**Профили групп доступа**» — настройка предустановленных шаблонов групп доступа пользователей. Профили групп доступа, как правило, объединяют в себе несколько ролей. При включении пользователя в группу доступа ему назначаются все роли, заданные в профиле группы доступа;
- «**Ограничивать доступ на уровне записей**» — при включенном флаге, активируется функционал «1С» по «**настройке RLS-ролей пользователей**». «RLS-роли» позволяют максимально гибко настраивать прав доступа пользователей к справочникам, документам и другим данным программы;
- «**Вариант работы**» — предлагается выбрать один из вариантов работы с RLS-ролями:
- «**Стандартный**» — вариант работы с RLS-ролями, при котором расчет прав выполняется «на лету» непосредственно при доступе к данным. Соответственно, чем сложнее прикладная логика ограничения доступа, тем расчет прав выполняется медленнее, оказывая непосредственное влияние на скорость основных сценариев работы пользователей: просмотр списков, формирование отчетов, открытие документов;
- «**Производительный**» — данный вариант основан на предварительном расчете прав доступа. Он позволяет достичь высокой производительности запросов с RLS, так как добавляет простой и статический фрагмент к текстам запросов в ролях. За счет этого он также обеспечивает одинаково хорошую скорость работы при различной прикладной логике ограничений доступа. В то же время предварительный расчет прав доступа занимает некоторое время, поэтому изменения в правах вступают в силу с некоторой задержкой (незначительной в большинстве случаев). Этот вариант работы с RLS-ролями, рекомендуется выбирать для клиент-серверной информационной базы, где он значительно эффективнее стандартного варианта. Однако в многопользовательской файловой информационной базе он может ограничивать интенсивность одновременной работы нескольких пользователей, поэтому может потребоваться стандартный вариант. При этом если в файловой базе работает один пользователь, либо данные вводятся несколькими пользователями не интенсивно, то производительный вариант не накладывает каких-либо дополнительных ограничений и ускорит просмотр списков и формирование отчетов по сравнению со стандартным вариантом. Производительный вариант является предпочтительным.

По умолчанию установлен «Стандартный» вариант работы с RLS-ролями.
При установке варианта «Производительный» выводится предупреждение о том, что включение данного варианта произойдет после окончания первого обновления. Обновление можно запустить добавленной в форму ссылки «**Обновление доступа на уровне записей**».

Программа позволяет настроить доступ пользователей к различным функциям, спискам и документам. Предусмотрены предопределенные наборы ролей. Кроме этого, имеется

возможность самостоятельной настройки доступа. Управление доступом осуществляет администратор. При этом пользователь, назначенный ответственным в группе доступа, может изменять состав своей группы доступа.

Набор прав и возможности по их ограничению определяются заданным профилем групп доступа.
Например, группа доступа «Менеджеры по продажам ПО делового назначения» с пользователями Иванов и Петров может ссылаться на профиль «Менеджер по продажам», в котором предусмотрена возможность ограничения по виду доступа «Виды номенклатуры». Тогда если по этому виду доступа для всех значений указать вариант «Запрещены», а в список добавить вид номенклатуры «ПО делового назначения», то Иванову и Петрову будут доступны только те данные и операции, которые связаны с ПО делового назначения.

Рекомендуется задавать наименования групп таким образом, чтобы название отражало как суть профиля, так и смысл ограничений, заданных в группе.

В состав группы доступа могут быть включены как отдельные пользователи (внешние пользователи), так и группы пользователей (группы внешних пользователей). В случае большого количества пользователей, участвующих сразу в нескольких группах доступа, рекомендуется объединять пользователей в группы. Включение таких групп пользователей в группы доступа позволит избежать рутинного пересмотра состава пользователей в нескольких группах доступа.

Состав ролей пользователя

Состав ролей пользователя определяется программой автоматически, исходя из того, в какие группы доступа он входит явно или косвенно (посредством групп пользователей), и обновляется каждый раз при изменении состава группы доступа или состава группы пользователей (группы внешних пользователей).

Не рекомендуется изменять состав ролей пользователей каким-либо другим способом (например, с помощью Конфигуратора), т.к. в этом случае состав ролей будет восстановлен при очередной записи группы доступа.

Объединение прав доступа

Пользователь может быть включен сразу в несколько групп доступа.

В этом случае его совокупные права доступа складываются (объединяются по «или») из прав доступа каждой группы. Например, в группе доступа «Менеджеры по закупкам» пользователю разрешен просмотр документов «Поступления товаров» по организации «Далекая перспектива». В группе доступа «Менеджеры по продажам» ему разрешен ввод документов «Заказ покупателя» по организации «Новые технологии».

При этом следует учитывать, что объединяются не списки разрешенных значений, указанные в группах, а именно права доступа. Т.е. ошибочно считать, что в приведенном примере пользователь получит доступ на просмотр документов поступления товаров и на ввод документов «**Заказы покупателей**» одновременно по обеим организациям.

From:
https://wiki.ilexx.ru/ - **Штрих-М: Документация**

Permanent link:
https://wiki.ilexx.ru/doku.php?id=tp7:%D0%B0%D0%B4%D0%BC%D0%B8%D0%BD%D0%B8%D1%81%D1%82%D1%80%D0%B8%D1%80%D0%BE%D0%B2%D0%B0%D0%BD%D0%B8%D0%B5:%D0%BD%D0%B0%D1%81%D1%82%D1%80_%D0%BF%D0%BE%D0%B8%D1%8C%D0%B7:%D0%B3%D1%80%D1%83%D0%BF%D0%BF%D1%8B_%D0%B4%D0%BE%D1%81%D1%82%D1%83%D0%BF%D0%B0

Last update: **2022/04/24 17:20**